PRESS RELEASE
www.fbbva.es

Press event with the three MIT researchers distinguished with the Frontiers of Knowledge Award in Information and Communication Technologies

Goldwasser, Micali and Rivest discuss how to protect citizens' security in the digital society without compromising privacy

- The work done by these mathematicians has laid the foundations of the cryptography field, with a vast impact in multiple areas of daily life in the new digital age: from the use of e-mail or social networks to online shopping by way of financial transactions
- Goldwasser explains that the technology is already in place to extract the fullest benefit from biomedical data without compromising their owners' privacy: "Different hospitals can share information on what treatments produce the best outcomes without identifying the patient whose information they are handling"
- Rivest declares himself skeptical about the security of electronic voting: "Right now, the safest bet is a paper ballot. I would not advise anyone to vote over the Internet"
- Micali, an expert in cryptocurrencies like Bitcoin, is convinced of their usefulness, but warns that "many of those around at the moment are not safe at all"

Madrid, 12 June 2018.- The question of how far we can go to preserve citizens' security without compromising their privacy has no easy answer: not even for the foremost authorities in cryptography. Shafi Goldwasser, Silvio Micali and Ronald Rivest, the three researchers distinguished with the Frontiers of Knowledge Award in the Information and Communication Technologies category, along with Israeli colleague Adi Shamir, engaged in a lively discussion this morning at a press conference prior to tomorrow's award presentation ceremony in the BBVA Foundation. The three are professors at Massachusetts Institute of Technology (MIT) in the United States. The award jury referred to them informally as "the guardians of privacy in the digital age."

For Goldwasser and Micali, cryptography offers reliable solutions to protect our personal data, while allowing law enforcement agencies to access them on a special-case basis, such as, for instance, intervening against a terrorist organization. “I am less optimistic,” says a more cautious Rivest, adding that “this is an active debate that will run for some time, because this is a complex, global problem. And, frankly, I see no solutions on the table that would allow us to decrypt messages to catch criminals without compromising everyone’s privacy; we are still a long way from that possibility.”

Goldwasser gives examples on how things might be done: “There are mathematical tools that would enable the police to access my key [to read my encrypted information] in determined situations”; for instance, if the encrypted message was a photograph featuring a listed terrorist.” The key could even be broken down – Micali adds – and the pieces distributed to trusted institutions, so it could only be reconstructed in special cases. Rivest, however, remains unconvinced: “We could go on and on with this discussion …”

The Frontiers of Knowledge Award was bestowed on them “for their fundamental contributions to modern cryptology, an area that has had a tremendous impact on our everyday life,” in the words of the jury’s citation. Their research, it continues, “has enabled the safe and secure transmission of electronic data, ranging from e-mail to financial transactions, (…) and provides the underpinning for digital signatures, blockchains and cryptocurrencies,” such as the well-known Bitcoin.

Rivest also prefers to err on the side of caution in an area that has recently occupied his research time: the security of electronic voting. “We tend to think that the latest technology is the best, but with electoral processes the newest technology simply isn’t reliable enough,” he remarks. “As we write, paper ballots are still the safest bet. I wouldn’t advise anyone to cast their vote over the Internet.”

Goldwasser offered some details of her recent research, focusing on how to maximally exploit data without invading the owners’ privacy. The aim is for different organizations to be able to share their data sets to harness the full power of the information they contain, without giving away the identities of the data owners. This is useful in many areas, for purposes like sharing genomic data in biomedicine, or results in the clinic: “Different hospitals can share information on what treatments produce the best outcomes without revealing the patient that information comes from,” she explains.

Micali, meantime, has devoted the last few years to the study of cryptocurrencies. While convinced of their utility, he also believes that “many of those around at the moment are not at all safe.” He is working on a new transactional platform with his company Algorand, seeking to address what he sees as the main flaws of Bitcoin and the other cryptocurrencies now in existence; among them, excess energy consumption and the strict centralization of currency issuance.

Authors of the first non-military encryption technique

In the late 1970s, encrypted information was essentially the sole domain of governments. In 1977, Rivest, Shamir and their MIT colleague Len Adleman – who would later abandon the cryptography field – devised a mathematical algorithm that, for the first time, placed encryption within reach of the general public. They baptized it with their combined initials, RSA, and before writing up the result in a specialist journal, published a partial account in *Scientific American*, offering to send the rest to anyone who requested it. The NSA (National Security Agency) attempted vainly to block the algorithm's distribution: however, by that time, the authors had received around 7,000 requests, and RSA had effectively fired the starting gun for modern cryptography. It remains in widespread use to this day, generally in combination with other techniques.

Since then Rivest and Shamir have continued contributing actively to the field's development. Rivest, specifically, created a popular algorithm with the ability to check that a given file – downloaded from the Internet, for instance – has not been tampered with.

Building trust while giving nothing away only the essentials

Goldwasser and Micali were students at the time the RSA method was published. Cryptography was by then a shared passion and their first contribution, during their doctoral studies, was to provide the mathematical demonstration that an encryption method is truly indecipherable.

This was the first of many seminal contributions. Goldwasser and Micali were co-authors of the "zero knowledge proof" showing that it is possible to convince an interlocutor of the truth of something without revealing what that something is: an algorithm that underlies applications ranging from authentication processes to Bitcoin transactions.

Laureate bio notes

Shafi Goldwasser

Shafrira Goldwasser (New York, USA, 1958) graduated in mathematics from Carnegie Mellon University, then went on to earn a PhD in Computer Science from the University of California, with a thesis on the theory and practice of probabilistic encryption. In 1983, she joined the Massachusetts Institute of Technology and by 1995 was a full professor, as well as co-leader with Ronald Rivest of the Cryptography and Information Security Group. Since 1997, she has held the RSA Professorship of Electrical Engineering and Computer Science, established that same year under an agreement with RSA Data Security, the firm set up by Ron Rivest, Adi Shamir and Leonard Adelman after developing the algorithm to which they lent their names.

She is also a member of the Theory of Computation Group and co-leads the Cryptography Group in the MIT Computer Science and Artificial Intelligence Laboratory. Since 1993, she has combined these responsibilities with the post of Professor of Computer Science and Applied Mathematics at the Weizmann Institute of Science (Israel), where she is a member of the Theory Group.

Silvio Micali

Silvio Micali (Palermo, Italy, 1954) graduated in mathematics from Sapienza University of Rome and earned a PhD degree in Computer Science from the University of California, Berkeley. In 1983 he joined MIT, where he is currently a full professor and associate head of the Department of Electrical Engineering and Computer Science. Like Rivest and Goldwasser, he works in the MIT Computer Science and Artificial Intelligence Laboratory.

His research focuses on information security. He has worked, like Adi Shamir, on the zero-knowledge proof and has been distinguished jointly with Shafi Goldwasser for his cryptographic research. Author of *Randomness and Computation* (from the series "Advances in Computing Research"), he has 47 patents to his name and is the founder of two companies: CoreStreet, providing smart credential software – acquired by ActiveIdentity in 2009 – and Peppercoin, which he set up with Ronald Rivest to market a cryptographic system for processing micropayments.

Ronald Rivest

Ronald Rivest (Schenectady, USA, 1947) holds a bachelor's degree in Mathematics from Yale University and a PhD in Computer Science from Stanford University. In 1974 he joined the Massachusetts Institute of Technology, where he is currently Institute Professor – the highest academic rank, held by fourteen of MIT's over one thousand faculty members – in the Department of Electrical Engineering and Computer Science.

Rivest is founder and currently co-leader with Shafi Goldwasser of the Cryptography and Information Security Group in the MIT Computer Science and Artificial Intelligence Laboratory. He is co-author of *Introduction to Algorithms*, a standard textbook in the subject area, and a past director of both the International Association for Cryptologic Research and the Financial Cryptography Association. He has founded three companies: RSA Data Security, Verisign – which came to be Internet's leading encryption, certification and authentication authority – and Peppercoin, in partnership with Silvio Micali.

More information

More background details on laureates and their contributions, video interviews and audios of the award announcement events with the winners' first declarations, are available on the Frontiers of Knowledge Awards website: https://www.premiosfronterasdelconocimiento.es/

Fundación BBVA

Para más información, puede ponerse en contacto con el Departamento de Comunicación de la Fundación BBVA (91 374 52 10; 91 374 31 39 y 91 374 81 73 o comunicacion@fbbva.es) o consultar en la web www.fbbva.es